

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-53185

(43) 公開日 平成11年(1999) 2月26日

(51) Int.Cl.<sup>6</sup>

G 0 6 F 9/06  
15/00

識別記号

5 5 0  
3 3 0

F I

G 0 6 F 9/06  
15/00

5 5 0 Z  
3 3 0 Z

審査請求 未請求 請求項の数6 O L (全 9 頁)

(21) 出願番号

特願平9-206493

(22) 出願日

平成9年(1997) 7月31日

(71) 出願人 000004226

日本電信電話株式会社

東京都新宿区西新宿三丁目19番2号

(72) 発明者 田中 利治

東京都新宿区西新宿三丁目19番2号 日本  
電信電話株式会社内

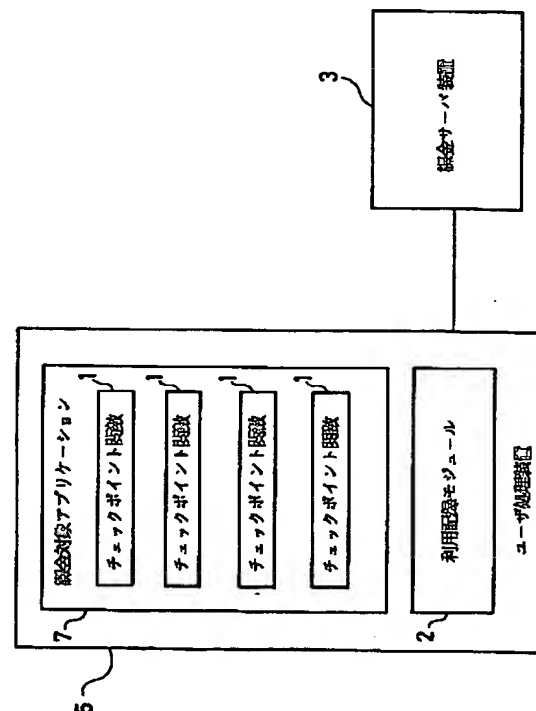
(74) 代理人 弁理士 三好 秀和 (外1名)

(54) 【発明の名称】 プログラムの機能単位利用量課金方法

(57) 【要約】

【課題】 ソフトウェアの使用機能に対応し、使用回数に比例した使用料の徴収を可能にするプログラムの機能単位利用量課金方法を提供する。

【解決手段】 課金対象アプリケーションの実行に先立ち、利用記録モジュール2はアプリケーション使用要求を課金サーバ装置3に送信し、課金サーバ装置は暗号鍵Kを利用記録モジュール2に送信し、課金対象アプリケーションの実行時にはチェックポイント関数1は起動毎に乱数 $R_1$ を生成し、該乱数を添付した起動通知を利用記録モジュールに通知し、利用記録モジュールは起動通知の回数を更新し、暗号鍵Kを用いて前記チェックポイント関数からの乱数 $R_1$ を暗号化し、この暗号化乱数をチェックポイント関数に返却し、チェックポイント関数は復号鍵 $K'$ を用いて利用記録モジュールからの暗号化乱数 $K(R_1)$ を復号化し、乱数 $R_1'$ と $R_1$ の一致を検証する。



## 【特許請求の範囲】

【請求項 1】 課金対象アプリケーションを有するユーザ処理装置に設けられた利用記録モジュールおよび前記ユーザ処理装置とネットワークを介して接続された課金サーバ装置を有するプログラム課金システムにおいて、課金対象アプリケーションは予め課金対象機能単位毎にチェックポイント関数が埋め込まれて配布され、前記チェックポイント関数は起動される毎に起動通知を前記利用記録モジュールへ通知し、前記利用記録モジュールは前記起動通知の回数を更新保持し、この保持した利用記録を前記課金サーバ装置に転送することを特徴とするプログラムの機能単位利用量課金方法。

【請求項 2】 前記チェックポイント関数は起動される毎に課金対象アプリケーションのプログラム識別情報を添付した起動通知を前記利用記録モジュールに通知し、前記利用記録モジュールはプログラム識別情報毎に起動通知の回数を更新保持し、この保持した利用記録を前記課金サーバ装置に転送することを特徴とする請求項 1 記載のプログラムの機能単位利用量課金方法。

【請求項 3】 前記チェックポイント関数は起動される毎に単価を添付した起動通知を前記利用記録モジュールに通知し、前記利用記録モジュールは単価の累積を更新保持し、この保持した利用記録を前記課金サーバ装置に転送することを特徴とする請求項 1 または 2 記載のプログラムの機能単位利用量課金方法。

【請求項 4】 前記チェックポイント関数には予め復号鍵  $K'$  が埋め込まれ、前記課金対象アプリケーションの実行に先立ち、前記利用記録モジュールはアプリケーション使用要求を前記課金サーバ装置に送信し、前記課金サーバ装置は前記復号鍵  $K'$  に対応する暗号鍵  $K$  を前記利用記録モジュールに送信し、前記利用記録モジュールは前記課金サーバ装置から受信した前記暗号鍵  $K$  を保持し、前記課金対象アプリケーションの実行時において、前記チェックポイント関数は起動される毎に乱数  $R_1$  を生成し、この生成した乱数  $R_1$  を添付した起動通知を前記利用記録モジュールに通知し、前記利用記録モジュールは起動通知の回数を更新保持し、前記暗号鍵  $K$  を用いて前記チェックポイント関数から受け取った前記乱数  $R_1$  を暗号化し、この暗号化した乱数  $K(R_1)$  を前記チェックポイント関数に返却し、前記チェックポイント関数は前記復号鍵  $K'$  を用いて前記利用記録モジュールから返却された前記暗号化された乱数  $K(R_1)$  を復号化し、この復号化した乱数  $R_1$  と前記生成された乱数  $R_1$  が一致していることを検証し、前記利用記録モジュールは保持した利用記録を前記課金

サーバ装置に転送することを特徴とする請求項 1 乃至 3 のいずれかに記載のプログラムの機能単位利用量課金方法。

【請求項 5】 前記チェックポイント関数には予め復号鍵  $K'$  が埋め込まれ、

前記課金対象アプリケーションの実行に先立ち、前記利用記録モジュールは前記課金対象アプリケーションのプログラム識別情報を添付して、アプリケーション使用要求を前記課金サーバ装置に送信し、

10 前記課金サーバ装置は前記プログラム識別情報で指定された前記課金対象アプリケーションに埋め込まれた前記復号鍵  $K'$  に対応する暗号鍵  $K$  を前記利用記録モジュールに送信し、

前記利用記録モジュールは前記課金サーバ装置から受信した前記暗号鍵  $K$  を前記プログラム識別情報と対にして保持し、

前記課金対象アプリケーションの実行時において、前記チェックポイント関数は起動される毎に乱数  $R_1$  を生成し、この生成した乱数  $R_1$  と課金対象アプリケーションのプログラム識別情報を添付した起動通知を前記利用記録モジュールに通知し、

20 前記利用記録モジュールはプログラム識別情報毎に起動通知の回数を更新保持し、前記プログラム識別情報に対応して前記暗号鍵  $K$  を用いて前記チェックポイント関数から受け取った前記乱数  $R_1$  を暗号化し、この暗号化した乱数  $K(R_1)$  を前記チェックポイント関数に返却し、

前記チェックポイント関数は前記復号鍵  $K'$  を用いて前記利用記録モジュールから返却された前記暗号化された乱数  $K(R_1)$  を復号化し、この復号化した乱数  $R_1$  と前記生成された乱数  $R_1$  が一致していることを検証し、

前記利用記録モジュールは保持した利用記録を前記課金サーバ装置に転送することを特徴とする請求項 1 乃至 3 のいずれかに記載のプログラムの機能単位利用量課金方法。

【請求項 6】 前記利用記録モジュールは前記課金サーバ装置の公開鍵  $K_s$  を保持し、また前記課金サーバ装置は課金サーバ装置自身の私的鍵  $K_s^{-1}$  を保持し、

40 前記利用記録モジュールは利用限度を保持し、前記チェックポイント関数の起動回数または単価累積が利用限度に到達すると、乱数  $R_2$  を生成し、この生成した乱数  $R_2$  と利用記録  $U$  を前記課金サーバ装置の公開鍵  $K_s$  を用いて暗号化し、この暗号化した情報  $K_s(R_2, U)$  を前記課金サーバ装置に送信し、

前記課金サーバ装置は前記利用記録モジュールから受信した前記暗号化情報  $K_s(R_2, U)$  を前記課金サーバ装置自身の私的鍵  $K_s^{-1}$  を用いて復号して前記乱数  $R_2$  と利用記録  $U$  を抽出し、前記課金サーバ装置が保持する課金情報を更新し、前記乱数  $R_2$  を前記課金サーバ装置

自身の私的鍵 $Ks^{-1}$ を用いて暗号化し、この暗号化した乱数 $Ks^{-1}(R_2)$ を前記利用記録モジュールへ送信し、

前記利用記録モジュールは前記課金サーバ装置から受信した前記暗号化乱数 $Ks^{-1}(R_2)$ を前記課金サーバ装置の公開鍵 $Ks$ を用いて復号し、この復号した乱数 $R_2'$ と前記生成した乱数 $R_2$ が一致していることを検証し、前記利用記録モジュール内に保持していた利用記録を削除することの特徴とする請求項1乃至3のいずれかに記載のプログラムの機能単位利用量課金方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、CD・ROMやフロッピーディスク等の媒体に格納されて配布されるソフトウェアや、ネットワークを介して配布されるソフトウェアに対して、機能単位の利用量に基づいて課金を行うプログラムの機能単位利用量課金方法に関する。

【0002】

【従来の技術】従来のソフトウェア課金システムには、ソフトウェアを販売し、ユーザが当該ソフトウェアを買い取った時点で課金が終了する方法がある。

【0003】また、ユーザが配布されたソフトウェアを利用する際に、課金センタに使用する旨を通知し、これにより、課金センタでは、ソフトウェアの使用に対する課金を行うシステムがある。

【0004】また、最近では、買い取り形式として暗号化されたソフトウェアをCD・ROM等の媒体、またはネットワーク経由で配布し、電話、ファクシミリ、手紙、または電子メールによる購入手続き後、復号鍵を通知する方式も採用されている。さらに、予め利用可能量が設定され、かつ暗号化されたソフトウェアを配布して、ユーザが使用した量を日数で管理し、当該日数に基づいて課金を行う方法等がある。

【0005】

【発明が解決しようとする課題】しかしながら、上記の買い取り方式では、流通経費を相対的に低減するためにソフトウェアの機能は肥大化し、ユーザは、殆ど使用しない機能を含め、高額のコストを負担しなければならない。また、ソフトウェアを購入して実行してみなければユーザが必要とする機能が満足されているか否かを判断できない。

【0006】また、単に、ユーザが配布されたソフトウェアを使用する際に、課金センタに使用する旨を通知する方法では、課金は可能であってもソフトウェアの使用を制限することができないため、使用料金の未払いがあっても対処することができないという問題がある。

【0007】暗号化されたソフトウェアを予め提供し、使用時に復号鍵を提供するシステムであっても、使用回数に関わらず、ユーザは、同一の金額を支払う必要があり、使用回数、または使用時間当たりの価格には大きな

幅がある。

【0008】本発明は、上記に鑑みてなされたもので、その目的とするところは、ソフトウェアの使用機能に対応し、使用回数に比例した使用料の徴収を可能にするプログラムの機能単位利用量課金方法を提供することにある。

【0009】

【課題を解決するための手段】上記目的を達成するため、請求項1記載の本発明は、課金対象アプリケーションを有するユーザ処理装置に設けられた利用記録モジュールおよび前記ユーザ処理装置とネットワークを介して接続された課金サーバ装置を有するプログラム課金システムにおいて、課金対象アプリケーションは予め課金対象機能単位毎にチェックポイント関数が埋め込まれて配布され、前記チェックポイント関数は起動される毎に起動通知を前記利用記録モジュールへ通知し、前記利用記録モジュールは前記起動通知の回数を更新保持し、この保持した利用記録を前記課金サーバ装置に転送することを要旨とする。

【0010】請求項1記載の本発明にあつては、課金対象アプリケーション内に課金対象機能単位毎に予め埋め込まれているチェックポイント関数は起動される毎に起動通知を利用記録モジュールへ通知し、利用記録モジュールは起動通知の回数を更新し、この利用記録を課金サーバ装置に転送するため、課金対象機能単位毎に実行回数に応じた課金が可能である。

【0011】また、請求項2記載の本発明は、請求項1記載の本発明において、前記チェックポイント関数は起動される毎に課金対象アプリケーションのプログラム識別情報を添付した起動通知を前記利用記録モジュールに通知し、前記利用記録モジュールがプログラム識別情報毎に起動通知の回数を更新保持し、この保持した利用記録を前記課金サーバ装置に転送することを要旨とする。

【0012】請求項2記載の本発明にあつては、チェックポイント関数は起動される毎に課金対象アプリケーションのプログラム識別情報を添付した起動通知を利用記録モジュールに通知し、利用記録モジュールはプログラム識別情報毎に起動通知の回数を更新し、この利用記録を課金サーバ装置に転送するため、プログラム識別情報を用いて課金対象アプリケーション毎に利用記録を集計することにより、課金対象機能単位の実行回数に応じて課金対象アプリケーションの権利保持者への利用料金支払いを行うことができる。

【0013】更に、請求項3記載の本発明は、請求項1または2記載の本発明において、前記チェックポイント関数は起動される毎に単価を添付した起動通知を前記利用記録モジュールに通知し、前記利用記録モジュールが単価の累積を更新保持し、この保持した利用記録を前記課金サーバ装置に転送することを要旨とする。

【0014】請求項3記載の本発明にあつては、チェッ

## 5

クポイント関数は起動される毎に単価を添付した起動通知を利用記録モジュールに通知し、利用記録モジュールは単価の累積を更新し、この利用記録を課金サーバ装置に転送するため、課金対象機能単位毎に単価を設定することにより、課金対象機能単位の開発工数、規模、ノウハウ、難易度、利用価値などにより課金対象機能単位毎に異なる料金を徴収することができる。

【0015】請求項4記載の本発明は、1乃至3のいずれかに記載の本発明において、前記チェックポイント関数には予め復号鍵 $K'$ が埋め込まれ、前記課金対象アプリケーションの実行に先立ち、前記利用記録モジュールがアプリケーション使用要求を前記課金サーバ装置に送信し、前記課金サーバ装置は前記復号鍵 $K'$ に対応する暗号鍵 $K$ を前記利用記録モジュールに送信し、前記利用記録モジュールが前記課金サーバ装置から受信した前記暗号鍵 $K$ を保持し、前記課金対象アプリケーションの実行時において、前記チェックポイント関数が起動される毎に乱数 $R_1$ を生成し、この生成した乱数 $R_1$ を添付した起動通知を前記利用記録モジュールに通知し、前記利用記録モジュールが起動通知の回数を更新保持し、前記暗号鍵 $K$ を用いて前記チェックポイント関数から受け取った前記乱数 $R_1$ を暗号化し、この暗号化した乱数 $K(R_1)$ を前記チェックポイント関数に返却し、前記チェックポイント関数は前記復号鍵 $K'$ を用いて前記利用記録モジュールから返却された前記暗号化された乱数 $K(R_1)$ を復号化し、この復号化した乱数 $R_1'$ と前記生成された乱数 $R_1$ が一致していることを検証し、前記利用記録モジュールが保持した利用記録を前記課金サーバ装置に転送することを要旨とする。

【0016】請求項4記載の本発明にあつては、チェックポイント関数で起動毎に乱数を生成して利用記録モジュールへ通知し、利用記録モジュールから返却された暗号化乱数を復号して元の乱数と比較検証するため、課金対象機能単位の実行回数に応じた利用記録が取得されることを保証することができる。

【0017】また、請求項5の本発明は、請求項1乃至3のいずれかに記載の本発明において、前記チェックポイント関数には予め復号鍵 $K'$ が埋め込まれ、前記課金対象アプリケーションの実行に先立ち、前記利用記録モジュールが前記課金対象アプリケーションのプログラム識別情報を添付して、アプリケーション使用要求を前記課金サーバ装置に送信し、前記課金サーバ装置が前記プログラム識別情報で指定された前記課金対象アプリケーションに埋め込まれた前記復号鍵 $K'$ に対応する暗号鍵 $K$ を前記利用記録モジュールに送信し、前記利用記録モジュールが前記課金サーバ装置から受信した前記暗号鍵 $K$ を前記プログラム識別情報と対して保持し、前記課金対象アプリケーションの実行時において、前記チェックポイント関数が起動される毎に乱数 $R_1$ を生成し、この生成した乱数 $R_1$ と課金対象アプリケーションのプロ

## 6

グラム識別情報を添付した起動通知を前記利用記録モジュールに通知し、前記利用記録モジュールがプログラム識別情報毎に起動通知の回数を更新保持し、前記プログラム識別情報に対応して前記暗号鍵 $K$ を用いて前記チェックポイント関数から受け取った前記乱数 $R_1$ を暗号化し、この暗号化した乱数 $K(R_1)$ を前記チェックポイント関数に返却し、前記チェックポイント関数が前記復号鍵 $K'$ を用いて前記利用記録モジュールから返却された前記暗号化された乱数 $K(R_1)$ を復号化し、この復号化した乱数 $R_1'$ と前記生成された乱数 $R_1$ が一致していることを検証し、前記利用記録モジュールが保持した利用記録を前記課金サーバ装置に転送することを要旨とする。

【0018】請求項5記載の本発明にあつては、チェックポイント関数で起動毎に乱数を生成して課金対象アプリケーションのプログラム識別情報とともに利用記録モジュールへ通知し、利用記録モジュールはプログラム識別情報毎に起動通知の回数を更新し、チェックポイント関数は利用記録モジュールから返却された暗号化乱数を復号して元の乱数と比較検証するため、課金対象機能単位の実行回数に応じた利用記録が取得されることを保証することができるとともに、プログラム識別情報を用いて課金対象アプリケーション毎に利用記録を集計することにより、課金対象機能単位の実行回数に応じて課金対象アプリケーションの権利保持者への利用料金支払いを行うことができる。

【0019】更に、請求項6記載の本発明は、請求項1乃至3のいずれかに記載の本発明において、前記利用記録モジュールが前記課金サーバ装置の公開鍵 $K_s$ を保持し、また前記課金サーバ装置は課金サーバ装置自身の私的鍵 $K_s^{-1}$ を保持し、前記利用記録モジュールが利用限度を保持し、前記チェックポイント関数の起動回数または単価累積が利用限度に到達すると、乱数 $R_2$ を生成し、この生成した乱数 $R_2$ と利用記録 $U$ を前記課金サーバ装置の公開鍵 $K_s$ を用いて暗号化し、この暗号化した情報 $K_s(R_2, U)$ を前記課金サーバ装置に送信し、前記課金サーバ装置が前記利用記録モジュールから受信した前記暗号化情報 $K_s(R_2, U)$ を前記課金サーバ装置自身の私的鍵 $K_s^{-1}$ を用いて復号して前記乱数 $R_2$ と利用記録 $U$ を抽出し、前記課金サーバ装置が保持する課金情報を更新し、前記乱数 $R_2$ を前記課金サーバ装置自身の私的鍵 $K_s^{-1}$ を用いて暗号化し、この暗号化した乱数 $K_s^{-1}(R_2)$ を前記利用記録モジュールへ送信し、前記利用記録モジュールが前記課金サーバ装置から受信した前記暗号化乱数 $K_s^{-1}(R_2)$ を前記課金サーバ装置の公開鍵 $K_s$ を用いて復号し、この復号した乱数 $R_2'$ と前記生成した乱数 $R_2$ が一致していることを検証し、前記利用記録モジュール内に保持していた利用記録を削除することを要旨とする。

【0020】請求項6記載の本発明にあつては、利用記

録モジュールから課金サーバ装置へ転送する利用記録および課金サーバ装置から利用記録モジュールへ転送する利用記録受取確認を公開鍵暗号化方式を用いて暗号化し、かつ利用記録および利用記録受取確認に毎回異なる乱数を生成して添付することにより、利用記録が課金サーバ装置へ確実に転送されたことを保証することができる。

#### 【0021】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態について説明する。

【0022】図1は、本発明の一実施形態に関わるプログラムの機能単位利用量課金方法を実施するシステムの構成を示す図である。同図においては、ユーザ処理装置5には予め課金対象機能単位毎にチェックポイント関数1が複数埋め込まれて配布された課金対象アプリケーション7が設けられ、また該課金対象アプリケーション7に隣接して利用記録モジュール2が設けられている。更に、ユーザ処理装置5はネットワークを介して課金サーバ装置3に接続されている。

【0023】図2は、図1に示すシステムを更に詳しく示したブロック図である。同図に示すように、チェックポイント関数1は、乱数を生成する乱数生成手段101、チェックポイント関数1の起動を利用記録モジュール2に通知する起動通知送信手段102、利用記録モジュール2から暗号化乱数を受信する暗号化乱数受信手段103、暗号化乱数を復号する復号手段104、およびこの復号した乱数と前記生成した乱数が一致していることを検証する乱数検出手段105を有する。

【0024】また、利用記録モジュール2は、課金対象アプリケーション7の使用要求を課金サーバ装置3へ送信する使用要求送信手段201、課金対象アプリケーション7に対応した暗号鍵を課金サーバ装置3から受信した暗号鍵受信手段202、前記暗号鍵を保持する暗号鍵保持手段203、チェックポイント関数1からの起動通知を受信する起動通知受信手段204、利用記録を管理する記録管理手段205、乱数および利用記録を暗号化する暗号化手段206、前記暗号化した乱数をチェックポイント関数1へ送信する暗号化乱数送信手段207、乱数を生成する乱数生成手段208、利用記録を課金サーバ装置3へ送信する利用記録送信手段209、課金サーバ装置3から暗号化乱数を受信する暗号化乱数受信手段210、前記暗号化乱数を復号する復号手段211、および該復号した乱数と前記生成した乱数が一致していることを検証する乱数検証手段212を有する。

【0025】更に、課金サーバ装置3は、課金対象アプリケーション7の使用要求を利用記録モジュール2から受信する使用要求受信手段301、課金対象アプリケーション7に対応した暗号鍵を利用記録モジュール2に送信する暗号鍵送信手段302、利用記録を利用記録モジュール2から受信する利用記録受信手段303、暗号化

された乱数および利用記録を復号する復号手段304、課金サーバ装置3内部に保持する課金情報を更新する課金情報更新手段305、乱数を暗号化する暗号化手段306、および暗号化した乱数を利用記録モジュール2に送信する暗号化乱数送信手段307を有する。

【0026】以上のように構成されるプログラムの機能単位利用量課金方法を実施するシステムにおいて、課金対象アプリケーション7の実行に先立ち、前記利用記録モジュール2は、使用要求送信手段201が課金対象アプリケーション7のプログラムIDを添付してアプリケーション使用要求を前記課金サーバ装置3へ送信する。前記課金サーバ装置3は、使用要求受信手段301がプログラムIDを添付されたアプリケーション使用要求を前記利用記録モジュール2から受信し、暗号鍵送信手段302が前記プログラムIDに対応して暗号鍵Kを前記利用記録モジュール2へ送信する。前記利用記録モジュール2は、暗号鍵受信手段202が前記暗号鍵Kを前記課金サーバ装置3から受信し、暗号鍵保持手段203が前記暗号鍵Kを保持する。

【0027】課金対象アプリケーションの実行中に、課金対象アプリケーション7の課金対象機能単位毎に埋め込まれた前記チェックポイント関数1が起動されると、前記チェックポイント関数1は、乱数生成手段101が乱数 $R_1$ を生成し、起動通知送信手段102が前記生成した乱数 $R_1$ と課金対象アプリケーションのプログラムIDと課金対象機能単位の単価とを添付した起動通知を前記利用記録モジュール2へ送信する。

【0028】前記利用記録モジュール2は、起動通知受信手段204が前記乱数 $R_1$ と前記プログラムIDと前記単価が添付された起動通知を前記チェックポイント関数1から受信し、記録管理手段205が前記プログラムIDに対応した単価累積を前記単価だけ更新し、暗号化手段206が前記暗号鍵保持手段203が保持する前記プログラムIDに対応した前記暗号鍵Kを用いて前記乱数 $R_1$ を暗号化し、暗号化乱数送信手段207が前記暗号化された乱数K( $R_1$ )を前記チェックポイント関数1へ送信する。

【0029】前記チェックポイント関数1は、暗号化乱数受信手段103が前記暗号化乱数K( $R_1$ )を前記利用記録モジュール2から受信し、復号手段104がチェックポイント関数1に予め埋め込まれた復号鍵K'を用いて前記暗号化乱数K( $R_1$ )を復号し、乱数検証手段105が前記復号された乱数 $R_1'$ と前記生成した乱数 $R_1$ が一致していることを検証する。

【0030】前記利用記録モジュール2の記録管理手段205が保持している単価累積が予め設定されている利用限度に到達すると、前記利用記録モジュール2は、乱数生成手段208が乱数 $R_2$ を生成し、暗号化手段206が利用記録モジュール2内に保持する前記課金サーバ装置3の公開鍵Ksを用いて前記生成した乱数 $R_2$ と記

録管理手段 205 が保持している利用記録  $U$  とを暗号化し、利用記録送信手段 209 が前記暗号化情報  $Ks(R_2, U)$  を前記課金サーバ装置 3 へ送信する。

【0031】前記課金サーバ装置 3 は、利用記録受信手段 303 が前記暗号化情報  $Ks(R_2, U)$  を前記利用記録モジュール 2 から受信し、復号手段 304 が課金サーバ装置 3 内に保持する課金サーバ装置自身の秘密鍵  $Ks^{-1}$  を用いて前記暗号化情報  $Ks(R_2, U)$  を復号して前記乱数  $R_2$  と前記利用記録  $U$  とを抽出し、課金情報更新手段 305 が前記利用記録  $U$  を用いて課金情報を更新し、暗号化手段 306 が前記秘密鍵  $Ks^{-1}$  を用いて前記乱数  $R_2$  を暗号化し、暗号化乱数送信手段 307 が前記暗号化乱数  $Ks^{-1}(R_2)$  を前記利用記録モジュール 2 へ送信する。

【0032】前記利用記録モジュール 2 は、暗号化乱数受信手段 210 が前記暗号化乱数  $Ks^{-1}(R_2)$  を前記課金サーバ装置 3 から受信し、復号手段 211 が前記公開鍵  $Ks$  を用いて前記暗号化乱数  $Ks^{-1}(R_2)$  を復号し、乱数検証手段 212 が前記復号された乱数  $R_2'$  と前記生成した乱数  $R_2$  が一致していることを検証し、記録管理手段 205 が前記利用記録  $U$  を削除する。

【0033】次に、図 3 乃至図 5 に示すフローチャートを参照して、詳細な作用を説明する。

【0034】図 3 は、本実施形態において課金対象アプリケーションの実行に先立つ準備段階における処理を示すフローチャートである。利用記録モジュール 2 は、使用要求送信手段 201 が課金対象アプリケーションのプログラム ID を添付したアプリケーション使用要求を課金サーバ装置 3 へ送信する（ステップ S11）。課金サーバ装置 3 は、使用要求受信手段 301 がプログラム ID を添付されたアプリケーション使用要求を利用記録モジュール 2 から受信し（ステップ S13）、暗号鍵送信手段 302 が前記プログラム ID に対応した暗号鍵  $K$  を利用記録モジュール 2 へ送信する（ステップ S15）。利用記録モジュール 2 は、暗号鍵受信手段 202 が前記暗号鍵  $K$  を課金サーバ装置 3 から受信し（ステップ S17）、暗号鍵保持手段 203 が前記暗号鍵  $K$  を保持する（ステップ S19）。

【0035】図 4 は、本実施形態において課金対象アプリケーションの実行中にチェックポイント関数が起動された時の処理を示すフローチャートである。チェックポイント関数 1 は、乱数生成手段 101 が乱数  $R_1$  を生成し（ステップ S21）、起動通知送信手段 102 が前記生成した乱数  $R_1$  と課金対象アプリケーションのプログラム ID と課金対象機能単位の単価とを添付した起動通知を利用記録モジュール 2 へ送信する（ステップ S23）。

【0036】利用記録モジュール 2 は、起動通知受信手段 204 が前記乱数  $R_1$  と前記プログラム ID と前記単価が添付された起動通知をチェックポイント関数 1 から

受信し（ステップ S25）、記録管理手段 205 が前記プログラム ID に対応した単価累積を前記単価だけ更新し（ステップ S27）、暗号化手段 206 が暗号鍵保持手段 203 が保持する前記プログラム ID に対応した前記暗号鍵  $K$  を用いて前記乱数  $R_1$  を暗号化し（ステップ S29）、暗号化乱数送信手段 207 が前記暗号化された乱数  $K(R_1)$  をチェックポイント関数 1 へ送信する（ステップ S31）。

【0037】チェックポイント関数 1 は、暗号化乱数受信手段 103 が前記暗号化乱数  $K(R_1)$  を利用記録モジュール 2 から受信し（ステップ S33）、復号手段 104 がチェックポイント関数 1 に予め埋め込まれた復号鍵  $K'$  を用いて前記暗号化乱数  $K(R_1)$  を復号し（ステップ S35）、乱数検証手段 105 が前記復号された乱数  $R_1'$  と前記生成した乱数  $R_1$  が一致していることを検証する（ステップ S37）。

【0038】図 5 は、本実施形態において利用記録モジュール 2 の記録管理手段 205 が保持している単価累積が予め設定されている利用限度に到達した時の処理を示すフローチャートである。利用記録モジュール 2 は、乱数生成手段 208 が乱数  $R_2$  を生成し（ステップ S41）、暗号化手段 206 が利用記録モジュール 2 内に保持する課金サーバ装置 3 の公開鍵  $Ks$  を用いて前記生成した乱数  $R_2$  と記録管理手段 205 が保持している利用記録  $U$  とを暗号化し（ステップ S43）、利用記録送信手段 209 が前記暗号化情報  $Ks(R_2, U)$  を課金サーバ装置 3 へ送信する（ステップ S45）。

【0039】課金サーバ装置 3 は、利用記録受信手段 303 が前記暗号化情報  $Ks(R_2, U)$  を利用記録モジュール 2 から受信し（ステップ S47）、復号手段 304 が課金サーバ装置 3 内に保持する課金サーバ装置自身の秘密鍵  $Ks^{-1}$  を用いて前記暗号化情報  $Ks(R_2, U)$  を復号して前記乱数  $R_2$  と前記利用記録  $U$  とを抽出し（ステップ S49）、課金情報更新手段 305 が前記利用記録  $U$  を用いて課金情報を更新し（ステップ S51）、暗号化手段 306 が前記秘密鍵  $Ks^{-1}$  を用いて前記乱数  $R_2$  を暗号化し（ステップ S53）、暗号化乱数送信手段 307 が前記暗号化乱数  $Ks^{-1}(R_2)$  を利用記録モジュール 2 へ送信する（ステップ S55）。

【0040】利用記録モジュール 2 は、暗号化乱数受信手段 210 が前記暗号化乱数  $Ks^{-1}(R_2)$  を課金サーバ装置 3 から受信し（ステップ S57）、復号手段 211 が前記公開鍵  $Ks$  を用いて前記暗号化乱数  $Ks^{-1}(R_2)$  を復号し（ステップ S59）、乱数検証手段 212 が前記復号された乱数  $R_2'$  と前記生成した乱数  $R_2$  が一致していることを検証し（ステップ S61）、記録管理手段 205 が前記利用記録  $U$  を削除する（ステップ S63）。

【0041】

【発明の効果】以上説明したように、本発明によれば、

課金対象アプリケーション内に課金対象機能単位毎に予め埋め込まれているチェックポイント関数は起動される毎に起動通知を利用記録モジュールへ通知し、利用記録モジュールは起動通知の回数を更新し、この利用記録を課金サーバ装置に転送するので、課金対象機能単位毎に実行回数に応じた課金が可能である。

【0042】また、本発明によれば、チェックポイント関数は起動される毎に課金対象アプリケーションのプログラム識別情報を添付した起動通知を利用記録モジュールに通知し、利用記録モジュールはプログラム識別情報毎に起動通知の回数を更新し、この利用記録を課金サーバ装置に転送するので、プログラム識別情報を用いて課金対象アプリケーション毎に利用記録を集計することにより、課金対象機能単位の実行回数に応じて課金対象アプリケーションの権利保持者への利用料金支払いを行うことができる。

【0043】更に、本発明によれば、チェックポイント関数は起動される毎に単価を添付した起動通知を利用記録モジュールに通知し、利用記録モジュールは単価の累積を更新し、この利用記録を課金サーバ装置に転送するため、課金対象機能単位毎に単価を設定して、課金対象機能単位の開発工数、規模、ノウハウ、難易度、利用価値などにより課金対象機能単位毎に異なる料金を徴収することができる。

【0044】本発明によれば、チェックポイント関数で起動毎に乱数を生成して利用記録モジュールへ通知し、利用記録モジュールから返却された暗号化乱数を復号して元の乱数と比較検証するので、課金対象機能単位の実行回数に応じた利用記録が取得されることを保証することができる。

【0045】また、本発明にあつては、チェックポイント関数で起動毎に乱数を生成して課金対象アプリケーションのプログラム識別情報とともに利用記録モジュールへ通知し、利用記録モジュールはプログラム識別情報毎に起動通知の回数を更新し、チェックポイント関数は利用記録モジュールから返却された暗号化乱数を復号して元の乱数と比較検証するので、課金対象機能単位の実行回数に応じた利用記録が取得されることを保証できるとともに、プログラム識別情報を用いて課金対象アプリケーション毎に利用記録を集計することにより、課金対象機能単位の実行回数に応じて課金対象アプリケーションの権利保持者への利用料金支払いを行うこ

とができる。

【0046】更に、本発明によれば、利用記録モジュールから課金サーバ装置へ転送する利用記録および課金サーバ装置から利用記録モジュールへ転送する利用記録受取確認を公開鍵暗号化方式を用いて暗号化し、かつ利用記録および利用記録受取確認に毎回異なる乱数を生成して添付するので、利用記録が課金サーバ装置へ確実に転送されたことを保証することができる。

【図面の簡単な説明】

10 【図1】本発明の一実施形態に係わるプログラムの機能単位利用量課金方法を実施するシステムの構成を示す図である。

【図2】図1に示すシステムを更に詳しく示したブロック図である。

【図3】図1に示す実施形態において課金対象アプリケーションの実行に先立つ準備段階における処理を示すフローチャートである。

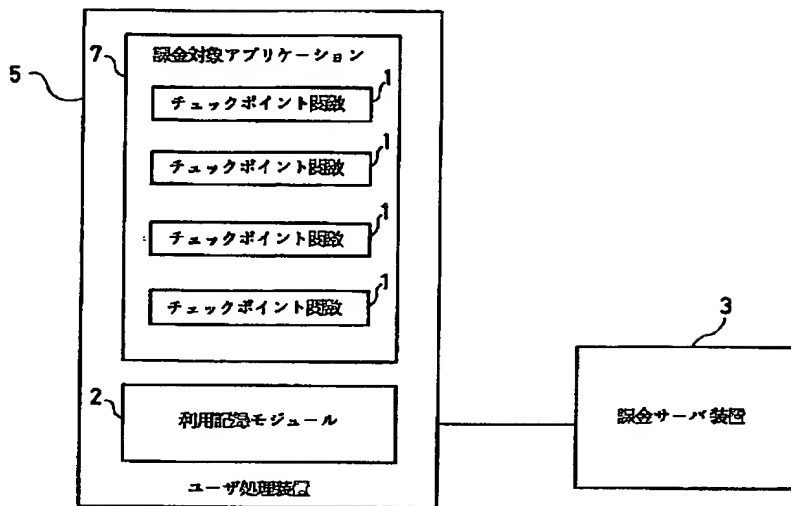
20 【図4】図1に示す実施形態において課金対象アプリケーションの実行中にチェックポイント関数が起動された時の処理を示すフローチャートである。

【図5】図1に示す実施形態において利用記録モジュールの記録管理手段が保持している単価蓄積が予め設定されている利用限度に到達した時の処理を示すフローチャートである。

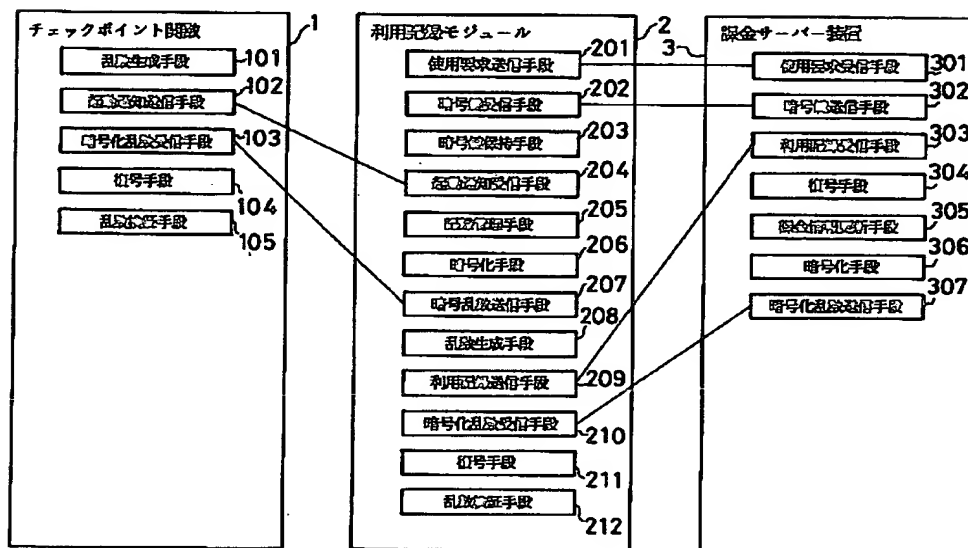
【符号の説明】

- 1 チェックポイント関数
- 2 利用記録モジュール
- 3 課金サーバ装置
- 5 ユーザ処理装置
- 30 7 課金対象アプリケーション
- 101 乱数生成手段
- 102 起動通知送信手段
- 105 乱数検証手段
- 201 使用要求送信手段
- 202 暗号鍵受信手段
- 204 起動通知受信手段
- 205 記録管理手段
- 209 利用記録送信手段
- 212 乱数検証手段
- 40 301 使用要求受信手段
- 302 暗号鍵送信手段
- 307 暗号化乱数送信手段

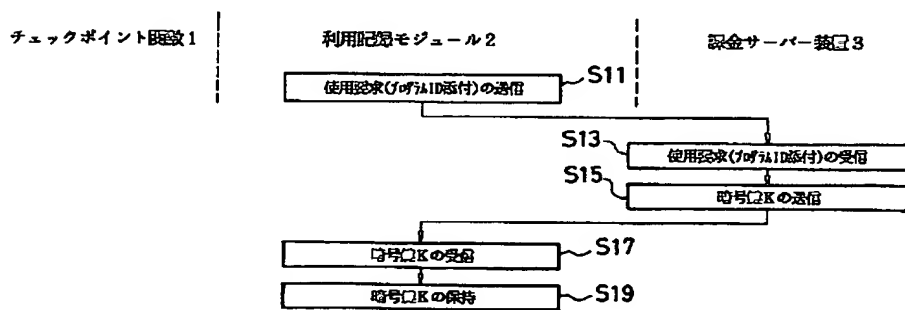
【図1】



【図2】

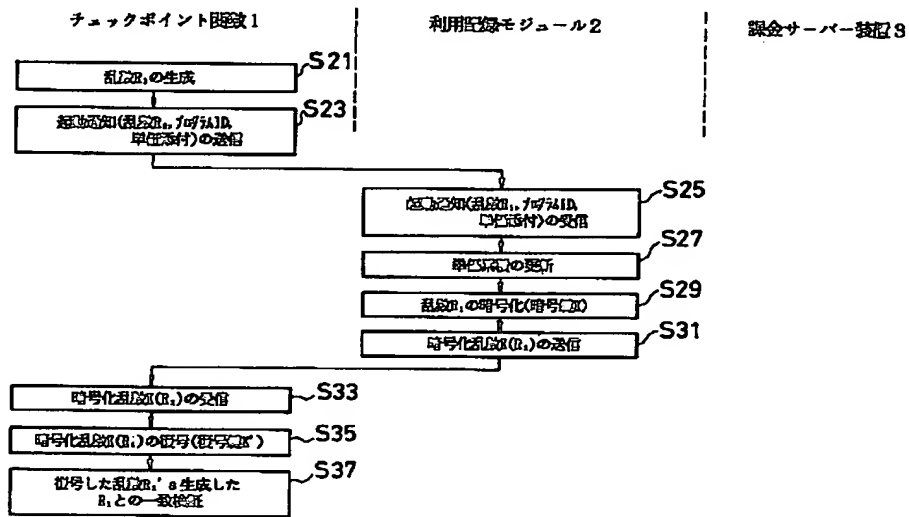


【図3】





【図4】



【図5】

